Underground Economies

Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency

McAfee | SAIC

Underground Economies:

Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency

Contents

Foreword	3
Introduction	5
Section 1 : The Changing Economy and the Value of Intellectual Capital	6
Section 2 : The Protection of Sensitive Data	9
Section 3 : Cyber Threats and the Increasing Impact on Business	14
Section 4 : Solutions and Policies Go Hand-in-Hand	16
Conclusion	18

Foreword by Simon Hunt, VP and CTO, Endpoint Security, McAfee

Globalization and the commoditization of information technology have driven businesses to store increasing amounts of precious corporate data in the cloud. As this shift has taken place, cybercriminals have discovered new ways to target this precious data, both from inside and outside the organization.

In the past, cybercriminals targeted personal information such as credit cards and social security numbers, which were then sold on the black market. Now, these criminals understand that there is much greater value in selling a company's proprietary information to competitors and foreign governments. For example, a company's legal documents can fetch far more money than a list of customer credit cards.

The cyber underground economy has shifted its focus to the theft of corporate intellectual capital–the new currency of cybercrime. Intellectual capital encompasses all the value that a company derives from its intellectual property including trade secrets, marketing plans, research and development findings and even source code. For example, Operation Aurora, a targeted attack on Google and at least 30 other companies, represented a sophisticated attack designed to steal intellectual capital.

More recently, we discovered the 'Night Dragon' attacks on oil and gas companies around the world, which over a period of several months silently and insidiously exfiltrated gigabytes of highly sensitive internal information including proprietary information about field operations, project financing and bidding documents. While these attacks focused specifically on the energy sector, the tools and techniques used can be highly successful when targeting any industry.

Data protection solutions are now more critical than ever as threats are coming from inside and outside the business. WikiLeaks, for example, poses a new threat to businesses, as insiders will be increasingly tempted to release their company's secrets for financial or technological gain, to increase the level of transparency of organizations, or to expose what they believe is wrongdoing. The spate of recent publicity around WikiLeaks has caused companies to take a serious look at what is confidential, what should be public and what should be protected. With the perimeter continuing to dissolve due to enterprises extending operations to mobile devices, cloud computing, and to third party providers, containing intrusion vectors is getting more and more difficult. Once exploitation of the network has been completed, the underground economy is very good at exfiltrating and monetizing the data.

While IT security investments are rising to prevent these intellectual capital thefts, so is the sophistication of the attacks, requiring advanced technologies and solutions to mitigate threats, in addition to training and policies. Having policies in place is important, but policies alone are not solving the problem.

This report evaluates the global corporate state of security, which is seemingly unprepared to protect itself from the sophistication of attacks generated by the underground economy. Have organizations adjusted their policies and approaches accordingly? The report concludes with approaches for protecting intellectual capital in order to stem losses and take full advantage of the coming economic recovery.

Introduction

Two years ago, McAfee produced the Unsecured Economies report, the first global study on the security of information economies. That study found that based on a global survey of businesses, companies worldwide lost more than an estimated $1 trillion in 2008 due to data leaks, the cost of remediation and reputational damage. Today, as the world economy begins to recover, businesses around the world are taking a renewed look at their intellectual capital, and how much is lost due to data loss and cyber attacks. Intellectual capital encompasses all the value that a company derives from its intellectual property including trade secrets, marketing plans, research and development findings and source code.

The Internet has crushed geographical boundaries, and companies have much of their value in intangible information that is stored in the cloud. As cybercriminals look for new information to steal, they look at issues such as overseas storage, which has made intellectual capital theft more prevalent and prosecution much more difficult. Often, companies are not even aware their information is being stolen due to the sophistication of the types of techniques used.

Although geography and culture can play a part, particularly in countries where the lines between business and government are blurred, it is the value of the data that determines who and what is attacked. The target and motivation are almost always financial.

In 2011, many questions will be similar to those asked two years ago, but the economic recovery, as opposed to an economic downturn makes the context different. How will an economic recovery impact the ability of organizations to protect vital information?

Which countries will pose the biggest threat to economic stability in other countries? How will cybercriminals target enterprises across all geographies? How will the protection of digital assets help or hinder a global economic recovery in the coming year?

In collaboration with experts in the fields of data protection and intellectual property, McAfee and Science Applications International Corporation (SAIC), a FORTUNE 500® scientific, engineering, and technology applications company, took a hard look at these questions.

Through a survey of more than 1,000 senior IT decision makers in the U.S., U.K., Japan, China, India, Brazil and the Middle East, McAfee together with SAIC developed a study on this topic. The survey, conducted by international research firm Vanson Bourne, reveals the changes in attitudes and perceptions of intellectual property protection in the last two years.

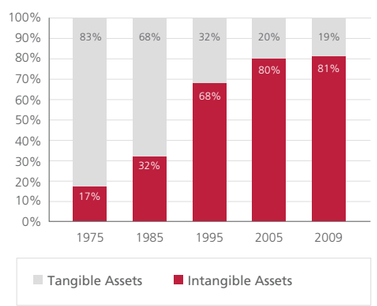
"Anything that can be monetized can become a target of the underground economy. These range from banking credentials of individuals to database dumps of Fortune 100 companies."

Marcel van den Berg, Team Cymru

Section 1: The Changing Economy and the Value of Intellectual Capital

The economy has made a shift in the last twenty years, from physical assets being the primary representation of value, to intellectual capital making up the bulk of corporate value. Recent analysis from Ocean Tomo Intellectual Capital Equity estimates the value of intangibles at around 81% of S&P 500 companies' value – a significant portion of which is represented by patented technology, trade secrets, proprietary data, business processes and go to market plans.

Components of S&P 500 Market Value



SOURCE: OCEAN TOMO

It is often hard to put a value on intellectual capital because it is rarely appraised, benefits from sometimes years of direct and indirect investment, and the underground economy's demand provides a price that often inaccurately reflects the worth to the company to which it belongs. For example, today's formula for Coke may not be as valuable to a competitor as what the Coca-Cola corporation's plan is for its new product line-up. What is a few million dollars if a competitor company can save billions in research and development by stealing Coke's proprietary data? Team Cymru's Marcel van den Berg frames the threat this way: "Anything that can be monetized can become a target of the underground economy. These range from banking credentials of individuals to database dumps of Fortune 100 companies."

In some cases, governments are supporting the theft of trade secrets, and in some countries the lines between business and government are blurred. If R&D costs are minimal or non-existent, companies can bring products to market faster, and make great profits off another company's investments. The theft of intellectual capital can lead to death by a thousand cuts to a corporation, and businesses worldwide should be concerned.

In 2009, German official Walter Opfermann, an espionage protection expert in the office for counter-intelligence for the state of Baden-Württemberg, said that China was using an array of "polished methods" from old-fashioned spies to phone-tapping, and increasingly the Internet, to steal industrial secrets[1]. The sectors most under attack included car manufacturing, renewable energies, chemistry, communication, optics, x-ray technology, machinery, materials research and armaments. Cybercriminals gather information on research and development, management techniques and marketing strategies.

The theft of intellectual capital can lead to death by a thousand cuts to a corporation, and businesses worldwide should be concerned

In Italy in September 2010, former Ferrari engineer Nigel Stepney was sentenced to 20 months in prison for his role in leaking of confidential corporate data in 2007. Stepney was found guilty of "sabotage, industrial espionage, sporting fraud and attempted serious injury," for having passed Ferrari's technical data to the rival McLaren racing team[2].

Intellectual capital is increasingly vulnerable due to the convergence of business and IT. Trade secrets and proprietary data reside in databases and are shared via email and the Internet. The targets for the underground economy have shifted significantly in the last couple of years. While it remains a profitable enterprise to buy and sell stolen credit cards, lately, intellectual capital has become the new source of large and easy pay-outs.

Indeed, the vectors and targets of virtual attacks on today's networked information society are multiplying. The High Technology Crimes Committee of the Brazilian Bar Association – São Paulo Chapter, summarizes: "We are seeing groups who specialize in rendering networks, services and basic infrastructure unavailable using more sophisticated (DDoS) attacks, causing lost revenue and damage to the image of major corporations. On the other hand, there are groups focused on surveying sensitive information and industrial espionage. Government data leaks will be a constant."

Today, cybercriminals care about content for profit and they can move quickly and flexibly to meet their goals. Once a vulnerability is identified, they can put a large operation into place within days of its discovery. They develop an exploit and steal as much useful data as possible in a short period. Mules are then used to send the profits (after taking a commission) to the leaders of the underground.

The economics of data storage abroad is playing a greater role in data decisions, as storing data abroad becomes cheaper and companies see the benefit that it can have on the bottom line. More than half of organizations studied are reassessing the risks of processing data outside of their home country due to the economic downturn, compared to four in ten doing so in 2008.

Email artifacts describing corporate culture, employee manuals and patents are the least protected type of data. A quarter or more of organizations report they are allocating very little or no budget to protecting this data. Client/supplier data, employee data and trade secrets are the best protected data though cyber attacks such as Operation Aurora (and others) prove that the most prized trade secrets are available to a sophisticated attacker despite traditional security protections.

Both the value of the information and the amount spent securing information has decreased in the last two years. In 2008, companies spent about $3 for the protection of $1 of data. This has proportionally increased to $4.80 in security for every $1 of data stored abroad because many companies have decreased the amount of data stored abroad while keeping the same protections. At the same time, approximately one third of organizations are looking to increase the amount of sensitive information they store abroad, up from one in five two years ago.

Some countries make it easier to store abroad given leniency in privacy and notification laws. Eight in ten organizations that store sensitive information abroad are influenced by privacy laws requiring notification of data breaches to customers. Seven in ten organizations that store sensitive information abroad do so in countries where laws give them more autonomy.

Decisions made in order to protect sensitive information are most often made in order to be compliant with the regulations in country. However, only a little more than a third of organizations feel that compliance regulations imposed by their home country are very useful and aim at the heart of the problem to protect their corporation's intellectual capital.

Approximately one third of organizations are looking to increase the amount of sensitive information they store abroad

Section 2: The Protection of Sensitive Data

There has been an evolution in the cyber underground, the type of data being attacked has changed, and as the attacks have become more sophisticated, the approach to data protection has changed as well. Not only do companies have to worry about competitors stealing intellectual capital, but they have to worry about sensitive or even classified information that could be leaked to media, as in the case of WikiLeaks.

In July, 2010, Gordon M. Snow, Assistant Director for the Federal Bureau of Investigation testified before House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security:

"The impact of cyber crime on individuals and commerce can be substantial, with the consequences ranging from a mere inconvenience to financial ruin. The potential for considerable profits is enticing to young criminals, and has resulted in the creation of a large underground economy known as the cyber underground. The cyber underground is a pervasive market governed by rules and logic that closely mimic those of the legitimate business world, including a unique language, a set of expectations about its members' conduct, and a system of stratification based on knowledge and skill, activities, and reputation."

The persistence and sophistication of the new threats is significant, and the attacks are taking place worldwide. In November 2010, Postmedia News reported that 86 percent of large Canadian corporations had been attacked, according to a secret report by the Canadian government. The report also said that espionage hacking of the private sector has doubled in two years.

A March 2010 Forrester Research report found that proprietary knowledge and company secrets are twice as valuable as custodial data which refers to payment card information, and customer and medical data:

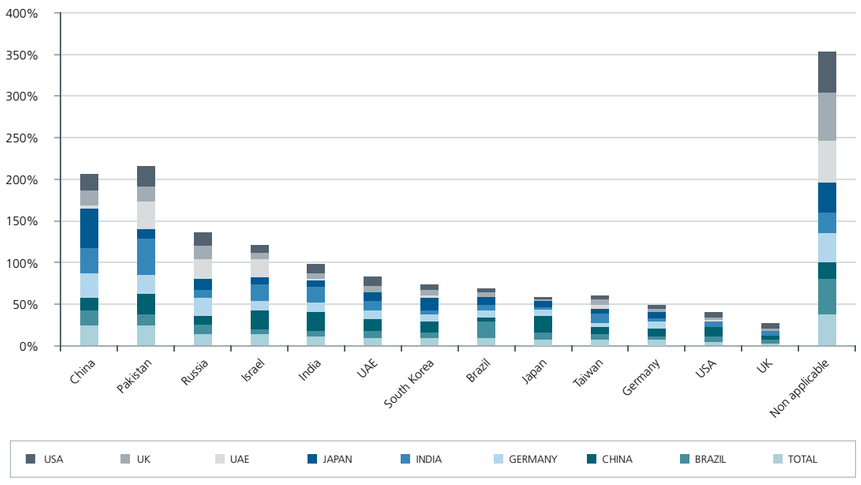
"Secrets comprise two-thirds of the value of firms' information portfolios. Despite the increasing mandates enterprises face, custodial data assets aren't the most valuable assets in enterprise information portfolios. Proprietary knowledge and company secrets, by contrast, are twice as valuable as the custodial data. And as recent company attacks illustrate, secrets are targets for theft[3]."

"Policies are not audited often by their managers which opens up numerous windows of opportunity to carry out illegal actions."

The High Technology Crimes Committee of the Brazilian Bar Association – São Paulo Chapter

Despite the fact that almost nine in ten organizations that store sensitive information abroad conduct a formal risk analysis, an increase since 2008, companies still store data in high-risk countries. While attacks are hard to trace back to a specific country, China, Russia, Pakistan are perceived to be the least safe for data storage. These are the same three countries that were regarded to be the least safe in 2008. The countries that were regarded to be the safest in 2008 were the United Kingdom, Germany and the United States, and this remains the case in 2010.

Figure 1 – Has your company avoided doing business with these countries?



Many organizations do not assess threats and risks as often as they should. More than a quarter of organizations assess the threats or risks posed to their data twice a year or less often. More than half of organizations determine the frequency of these risk assessments on their own, rather than on auditor recommendations or regulatory requirements.

As The High Technology Crimes Committee of the Brazilian Bar Association – São Paulo Chapter, says: "The vast majority of companies from various industries lack the control of their information security policies and even groups from different corporate areas take time to discuss these events. In fact, policies are not audited often by their managers which opens up numerous windows of opportunity to carry out illegal actions. It seems as if corporate actions are not punished. Companies need to work on this image with ongoing training aimed at protecting their intellectual capital."

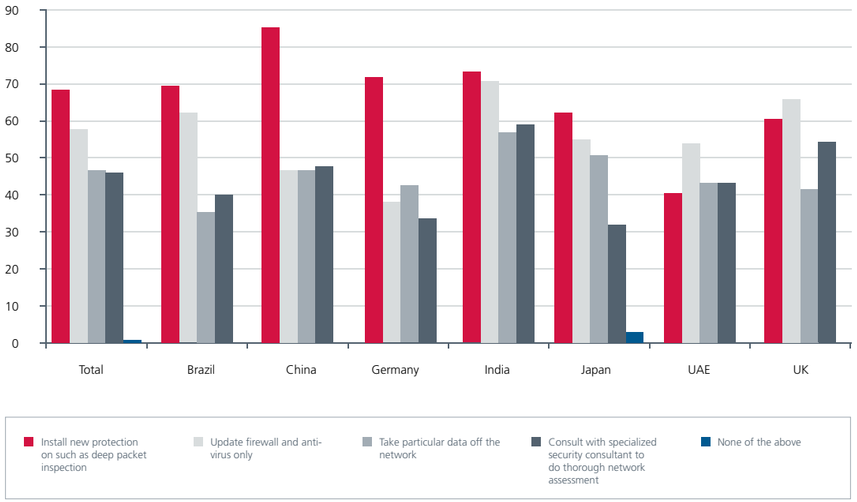
More than a quarter of organizations assess the threats or risks posed to their data twice a year or less often

In China, Japan, United Kingdom and the United States, organizations are on average spending more than $1 million a day on their IT

In China, Japan, United Kingdom and the United States, organizations are on average spending more than $1 million a day on their IT, and in United States, China and India, organizations are on average spending more than $1 million a week on securing sensitive information abroad. Approximately half of organizations surveyed are looking to increase their IT security spending on hardware upgrades, software upgrades and external hosting of data and other services. Around half of organizations anticipate that their investment in securing sensitive information will increase, with only one in twenty looking to decrease their spending.

Despite growth of IT security spending, the solutions are often reactive. When steps are taken, organizations are most likely to install new protection such as deep packet inspection, as reported by more than two-thirds of respondents. The most popular method of protecting sensitive data is through the use of anti-virus software, firewalls and intrusion detection/prevention (IDS/IPS) systems, implemented by more than four in five organizations.

Figure 2 – What steps are taken to remediate and protect systems for the future?

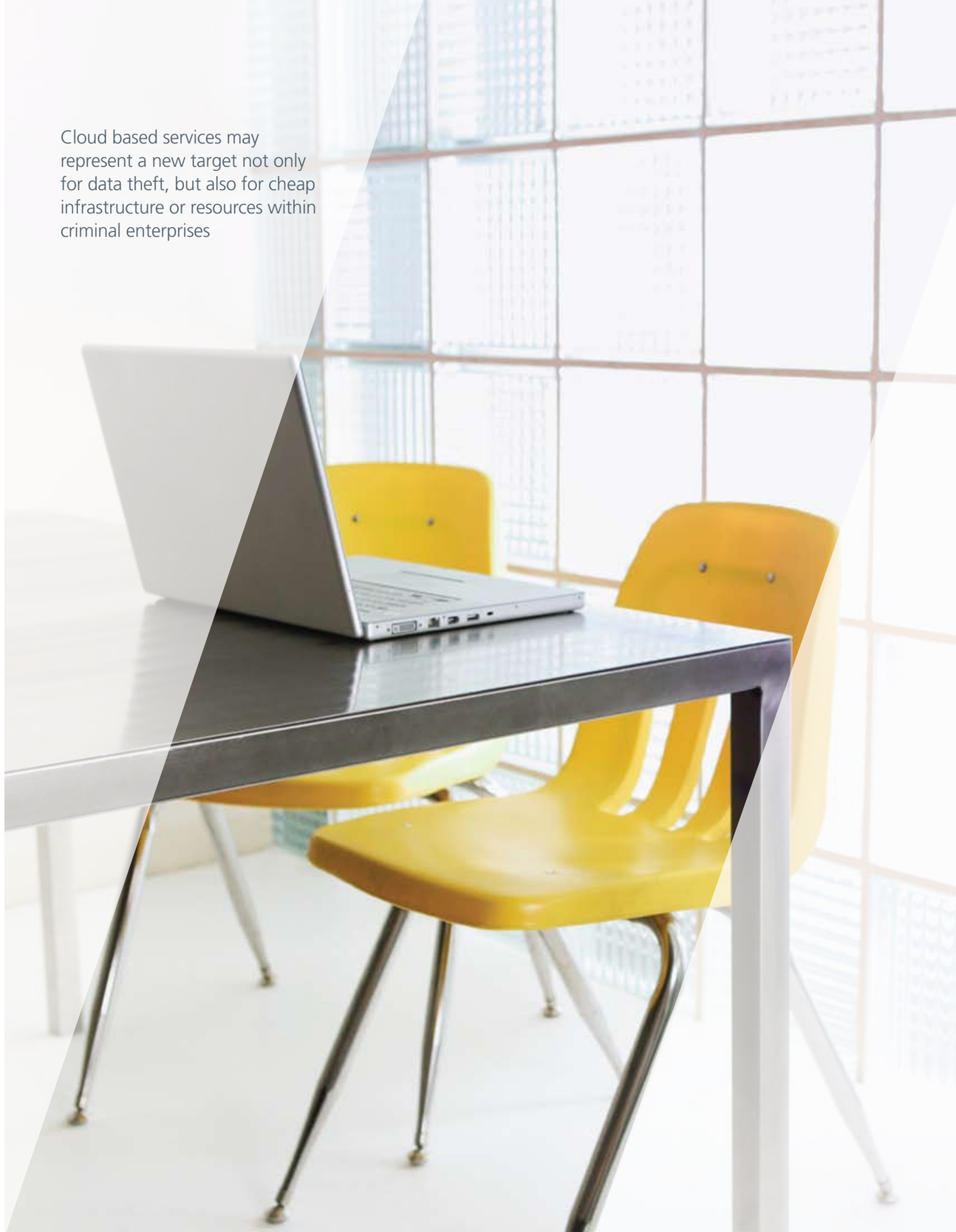


It is noteworthy, that almost half of respondents reported that they would "take particular data off the network" in order to protect it from being leaked. Here the security of the data is considered to be more important to the organization than the availability or usage of the data.

Securing mobile devices continues to pose a challenge to businesses with 62 percent of respondents identifying this as challenge. The greatest challenge organizations face when managing information security is the changing nature of attacks, followed very closely by the proliferation of devices and services, such as removable media, smart phones, and social networking sites. Mobility continues to empower and enable workforces to accomplish more than ever, and this trend is only increasing. Simultaneously, social media channels are of growing interest for businesses to leverage. These two forces represent an astronomical increase in the level of risk organizations face with regard to leaked data. This coupled with an organizations' need to share critical data with key partners means the traditional approach to cyber security needs to be augmented. "Smart phones will most likely cause an increase in criminal research and development efforts due to their ubiquity and functionality. Cloud based services may also represent a new target not only for data theft, but also for cheap infrastructure or resources within criminal enterprises," says Team Cymru's Marcel van den Berg.

Securing mobile devices continues to pose a challenge to businesses with 62 percent of respondents identifying this as challenge

Cloud based services may represent a new target not only for data theft, but also for cheap infrastructure or resources within criminal enterprises



Section 3: Cyber Threats and the Increasing Impact on Business

Media coverage has increased concerns about the loss of confidential information, especially by insiders. In 2008, three people were convicted for stealing marketing plans from Coca-Cola[4] and a year later, a former Goldman Sachs computer programmer was arrested for stealing computer code used to perform proprietary trading[5].

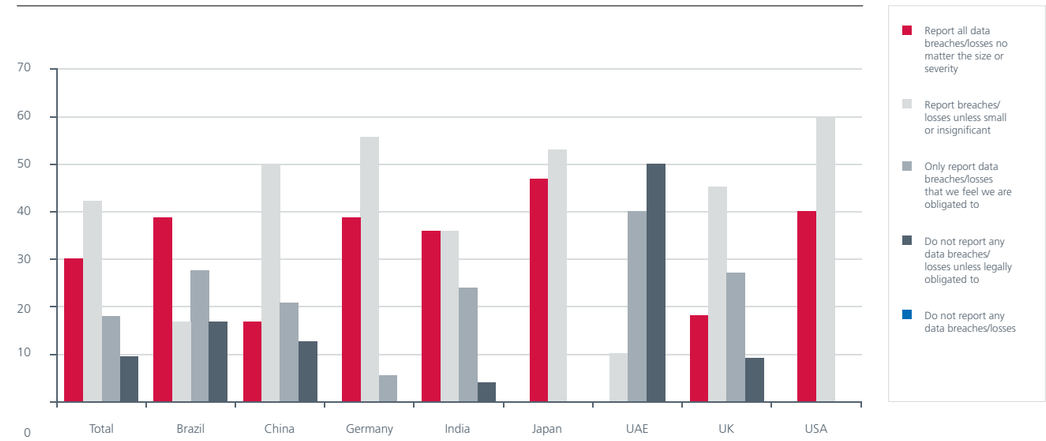
"A single mistake by an unaware employee can have dire consequences," said Dinesh Pillai, chief executive officer, Mahindra Special Services Group, a leading corporate security risk consulting firm in India. "An employee socially engineered by an attacker could result in critical data leakage, financial and reputational losses or stall the business functionality of the company. Most of the current technologies use the preloaded algorithms to sense any anomaly. However the underground world is far superior in terms of their technology capability and skills and they can identify ways and means to break the systems."

Additionally, according to The High Technology Crimes Committee of the Brazilian Bar Association – São Paulo Chapter, the insider threat is often not just 'accidental': "Based on our assessment, the biggest threat inside are the professionals considered 'Intruders'. These professionals work in minor roles and carry out social engineering and sensitive data appropriation techniques.

"A number of companies put their direct and indirect employees under stricter scrutiny. In many cases, there are professionals who suffer pressure from criminal gangs in their underserved communities. These gangs ask employees for sensitive information, such as courier delivery dates, electronic stations, supply schedules, internal and external security passwords among other corporate information, in exchange for the safety of their families."

As a result, just as in the previous study, reputational impact worries organizations the most. Around half of organizations reported that as their number one concern regarding a data breach involving sensitive information or intellectual property. Today a public company can lose a top-secret recipe, a go-to-market plan or other key secret and they are reluctant to report it given the potential backlash from customers, shareholders, and the market. Media coverage after a breach can affect brand reputation, and shareholder value and therefore are underreported.

Figure 3 – Reporting of data breaches



One in seven organizations has not reported data breaches and/or losses to outside government agencies or authorities, or stockholders. Only three in ten organizations report all data breaches/losses suffered, while one in ten organizations will only report breaches/losses that they are legally obliged to, and no more. Six in ten organizations currently "pick and choose" the breaches/losses they report, depending on how they feel about them.

The admission of a significant vulnerability could flag other attackers so very few companies are willing to be public about intellectual capital losses.

M&A activity, partnerships, product roll-outs are all potential victims of cyber theft and the miscreants of the underground economy. Around a quarter of organizations have had a merger and acquisition or a new product/solution rollout stopped or slowed by a data breach, or the credible threat of a data breach. Almost half of all organizations have experienced a small data breach, and almost a quarter of organizations have suffered a data breach in the last year, more than in 2008.

Data breaches are also expensive. On average, this lost/breached data costs organizations more than $1.2 million, compared to less than $700,000 in 2008.

Perhaps this is why only a quarter of organizations conduct forensic analysis of a breach or loss, and only half take steps to remediate and protect systems for the future after a breach or attempted breach. More than half of organizations have, at some point in their history, decided not to further pursue or investigate a security incident because of the cost of such an investigation/pursuit. Organizations are more likely to review/investigate a small data breach internally, rather than bringing in external help. This lack of investigation means that potential vectors of attack are not shored up and future penetration is possible or the threat persists. Insiders are not identified, and incongruities are not investigated to identify a larger threat. This lack of remediation may open up companies to the risks of future breaches.

The most significant threat reported by organizations when protecting their sensitive information was data leaked accidentally or intentionally by employees. Employees' adherence (or lack thereof) to security procedures is considered to be the greatest challenge to organizations' information security. This ranked higher than other challenges, including multiple systems within the organization or the insecurity of supply chain partner systems. Policies clearly have not stemmed the data leak, forcing the hand of corporations to choose robust and innovative technical solutions to reinforce their guidelines.

One in ten organizations will only report breaches/losses that they are legally obliged to, and no more

Section 4: Solutions and Policies Go Hand-in-Hand

For many companies, security and risk managementdecisions are based on strict adherence to compliance standards, not on protecting their intellectual capital. These companies often do not make the connection that the impact of a data breach can have a major impact on business and productivity, slowing down product development and interfering with M&A activity.

Policies must work hand in hand with advanced solutions in order to make a difference. They must be implemented along with technology for deep packet inspection, data loss prevention, advanced threat monitoring, forensics and even taking particular data off the network.

Furthermore, the distinction between insiders and outsiders is blurring. "Sophisticated attackers infiltrate a network, steal valid credentials on the network, and operate freely – just as an insider would. Having defensive strategies against these blended insider threats is essential, and organizations need insider threat tools that can predict attacks from this blended threat," said Scott Aken, Vice President for Cyber Operations at SAIC.

Tom Kellermann, Vice President of Security Awareness for Core Security Technologies, cites the lack of robust penetration testing and remediation timetables as a keyhole in many companies' cybersecurity strategies. Additionally, weak authentication, porous wireless security and insufficient wireless IDS technology contribute to the problem.

Kellermann says that incident response and forensics capabilities must be assessed regularly. "Specifically, the Advanced Persistent Threat illustrates the need for incident response to include attack path mapping. Third party managed service providers such as hosting companies and cloud infrastructure providers must be contractually bound to test their security posture and to adhere to higher standards of cybersecurity before they become "watering holes in East Africa" for predators to infiltrate," reports Kellermann.

"Most organizations are still looking at cybersecurity as a perimeter-based problem. With the perimeter continuing to expand through mobile devices and cloud computing, a cyber security department's job is getting tougher," added Aken.

Some emerging trends that are changing the ways companies are defying sophisticated attacks and insider leaks are listed below:

Deep Packet Inspection (DPI) – A DPI solution acts as a highly flexible complement to existing security architecture, performing inline, full packet (layers 2-7) analysis in near real-time of all packets (i.e., without packet loss). The software applications that lie on top of the hardware allow for any kind of rules-based arrangement to strip data off packets leaving a network as well as prevent any type of exploit by stripping it from incoming traffic.

Human Behavior Based Network Security – These are solutions that are a step ahead of the hackers or insiders that detect intent through the activities taken on the network. These solutions do not use signatures, anomalies, or heuristics, but human behaviors that are common to all deceptive actions on a network which can be stopped prior to having data leave a network.

Insider Threat Tools – Recent innovations in insider threat technologies have created tool suites that can be deployed on systems to monitor hundreds to thousands of inside users simultaneously, tracking their actions and identifying traits inherent in those actions that should be cause for alert. By profiling suspicious activities at line speed, these solutions can interrupt connections if data is inappropriately being removed or other unusual and critical operations are taking place.

Advanced Forensics – Every digital device, every computer, every mobile phone tells a story that is traceable through a trail of "digital DNA" uncovered through sophisticated computer and network analysis. Software tools and services help discover and extract critical content, and identify user behaviors and unique identifiers. Knowing which gaps and vulnerabilities led to an attack is the first step in preventing the next attack.

Advanced Malware Analysis – It is now possible to discover zero-day malware that will use or is using network exploits to attack a network. Once discovered, and the malware can be captured for analysis and response.

Conclusion

While cybersecurity holes cannot be eliminated completely, organizations can greatly reduce the risks associated with confidential data leaving their organizations. Organizations are looking for a way to monitor the movement of sensitive information and stop the potential loss of data via malicious intent or inadvertent release. This can all be prevented.

Appliances can be installed on the network to record and classify everything that goes over the Internet, and there are devices that can mine stored structured and unstructured data so organizations can search and discover where sensitive data is kept. While these devices are not new, they are continually being upgraded and incorporating more predictive capabilities based on human behavior. Solutions such as deep packet inspection, human behavioral analysis, and encryption are all solutions that will grow in use and effectiveness in the years to come.

Today, organizations are looking beyond "check-the-box" compliance, and looking to protect more sensitive data – like design documents, schematics, product launch plans, pharmaceutical formulas – their intellectual capital. These types of documents are much more complex than simple Social Security numbers or credit card numbers, and require advanced protection solutions.

Scott Aken believes that protection of the enterprise starts with education and understanding of what you are trying to protect.

"Most organizations spend enormous sums of money protecting the less critical portions of their network while the crown jewels, their intellectual capital, remain wide open. The thorough analysis of what lies on the network, combined with a solid Defense in Depth strategy, all implemented by a properly trained staff can do wonders for protecting an organization's data."

Contributors

Scott Aken, Vice President for Cyber Operations, SAIC

Jenifer George, Cyber Portfolio Manager, SAIC

Marcel van den Berg, Team Lead for Business Intelligence, Team Cymru

Simon Hunt, vice president and Chief Technology Officer, Endpoint Security, McAfee

Tom Kellermann, Vice President of Security Awareness for Core Security Technologies

Dinesh Pillai, Chief Executive Officer, Mahindra Special Services Group

Erasmo Ribeiro Guimarães Junior, Secretary and Member of The High Technology Crimes Committee at OAB-SP

Marco Aurélio Pinto Florêncio Filho, Vice Chairman of The High Technology Crimes Committee at OAB-SB

Coriolano Aurélio de Almeida Camargo Santos, Chairman of The High Technology Crimes Committee at OAB-SP

References:

1 *http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage*

2 *http://f1grandprix.motorionline.com/condannato-nigel-stepney-patteggia-1-anno-e-8-mesi/*

3 *http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf*

4 *http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf*

5 *http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aSDxSdMIPTXU*

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

www.mcafee.com

About SAIC

SAIC is a FORTUNE 500® scientific, engineering, and technology applications company that uses its deep domain knowledge to solve problems of vital importance to the nation and the world, in national security, energy and the environment, critical infrastructure, and health.

SAIC: From Science to Solutions®
For more information, visit www.saic.com

McAfee
2821 Mission College Blvd.,
Santa Clara, CA 95054
www.mcafee.com

The information in this document is provided only for education purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided 'AS IS' without guarantee or warranty as to the accuracy or applicability of the information to any specific situation of circumstance. McAfee and the McAfee logo are registered trademarks or trademarks of McAfee or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others. 2011 McAfee.